

# U.S. Department of Commerce

## U.S. Patent and Trademark Office



### Privacy Impact Assessment for the MicroPact Equal Employment System (EES)

Reviewed by: John B. Owens II, Bureau Chief Privacy Officer

Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer  
 Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer

**Catrina D. Purvis**



Digitally signed by Catrina D. Purvis  
DN: cn=Catrina D. Purvis, o=Office of the Secretary, Office of Privacy and Open  
Government, ou=US Department of Commerce, email=cpurvis@doc.gov, c=US  
Date: 2017.06.06 16:34:36 -04'00'

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer

Date

## **U.S. Department of Commerce Privacy Impact Assessment USPTO MicroPact Equal Employment System (EES)**

**Unique Project Identifier: [2428] PTOC-026-00**

### **Introduction: System Description**

*Provide a description of the system that addresses the following elements:*

*The response must be written in plain language and be as comprehensive as necessary to describe the system.*

#### *(a) a general description of the information in the system*

The EES system is an application information system, and provides support to the Office of Equal Employment Opportunity and Diversity business functions within the United States Patent and Trademark Office (USPTO). The EES supports all activities associated with the recruitment and management of USPTO personnel. The EES is composed of two (2) Information Systems that provide the following capabilities:

- Track and manage Equal Employment Opportunity (EEO) claims through the USPTO; and,
- The RA (Reasonable Accommodations) program housed in OEEOD includes processing requests and ensuring that RA requests are addressed promptly, thoroughly, and in strict compliance with the Equal Employment Opportunity Commission's (EEOC) regulations.

#### *(b) a description of a typical transaction conducted on the system*

### **The Reasonable Accommodation Case Management System (RACMS)**

RACMS is designed to help the Office of Equal Employment Opportunity and Diversity staff to process requests for reasonable accommodation by collecting and maintaining data on accommodations requested and provided, and costs of each accommodation, for annual reporting purposes. The Reasonable Accommodation Case Management System is using the MicroPact COTS product entellitrak. The entellitrak RA Edition and entellitrak efile COTS software is an electronic case management and tracking system to track the RA requests. The USPTO requires a software package to track and manage the flow of RA requests through the RA process from the initial filing of a new RA request to the final resolution of the request.

### **The Equal Employment Opportunity Case Management and Reporting System (EOCMRS)**

Equal Employment Opportunity Case Management and Reporting System (EOCMRS) is an Information System that supports the Office of Equal Employment Opportunity and

Diversity (OEEOD) of the United States Patent and Trademark Office. The mission of the EEOCMRS is to provide automated information support to the OEEOD in tracking and managing the flow of Equal Employment Opportunity (EEO) claims through the USPTO process. The EEOCMRS customer base consists of EEO staff in USPTO Headquarters. OEEOD staff is the primary users of the system. The EEOCMRS system is using the MicroPact COTS product iComplaints.

*(c) any information sharing conducted by the system*

Information stored and processed by the EES system is not shared outside of the approved user groups and USPTO business units for the system.

*(d) a citation of the legal authority to collect PII and/or BII*

The legal authority to collect PII for this system comes from the Department of Commerce SORN: *Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18.*

Legal authority citations include the following, with all revisions and amendments: 5 U.S.C. 301; 44 U.S.C. 3101; E.O. 12107, E.O. 13164, 41 U.S.C. 433(d); 5 U.S.C. 5379; 5 CFR Part 537; DAO 202–957; E.O. 12656; Federal Preparedness Circular (FPC) 65, July 26, 1999; DAO 210–110; Executive Order 12564; Public Law 100–71, dated July 11, 1987.

*(e) the Federal Information Processing Standard (FIPS) 199 security impact category for the system is **Moderate**.*

## **Section 1: Status of the Information System**

1.1 Indicate whether the information system is a new or existing system.

- This is a new information system.
- This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*
- This is an existing information system in which changes do not create new privacy risks. *Continue to answer questions, and complete certification.*

<b>Changes That Create New Privacy Risks (CTCNPR)</b>					
a. Conversions	<input type="checkbox"/>	d. Significant Merging	<input type="checkbox"/>	g. New Interagency Uses	<input type="checkbox"/>
b. Anonymous to Non-Anonymous	<input type="checkbox"/>	e. New Public Access	<input type="checkbox"/>	h. Internal Flow or Collection	<input type="checkbox"/>
c. Significant System Management Changes	<input type="checkbox"/>	f. Commercial Sources	<input type="checkbox"/>	i. Alteration in Character of Data	<input type="checkbox"/>
j. Other changes that create new privacy risks (specify):					

## **Section 2: Information in the System**

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

<b>Identifying Numbers (IN)</b>					
a. Social Security*	<input type="checkbox"/>	e. File/Case ID	<input checked="" type="checkbox"/>	i. Credit Card	<input type="checkbox"/>
b. Taxpayer ID	<input type="checkbox"/>	f. Driver's License	<input type="checkbox"/>	j. Financial Account	<input type="checkbox"/>
c. Employer ID	<input type="checkbox"/>	g. Passport	<input type="checkbox"/>	k. Financial Transaction	<input type="checkbox"/>
d. Employee ID	<input checked="" type="checkbox"/>	h. Alien Registration	<input type="checkbox"/>	l. Vehicle Identifier	<input type="checkbox"/>
m. Other identifying numbers (specify):					
*Explanation for the need to collect, maintain, or disseminate the Social Security number, including truncated form:					
*If SSNs are collected, stored, or processed by the system, please explain if there is a way to avoid such collection in the future and how this could be accomplished:					

<b>General Personal Data (GPD)</b>					
a. Name	<input checked="" type="checkbox"/>	g. Date of Birth	<input checked="" type="checkbox"/>	m. Religion	<input type="checkbox"/>
b. Maiden Name	<input type="checkbox"/>	h. Place of Birth	<input type="checkbox"/>	n. Financial Information	<input type="checkbox"/>
c. Alias	<input type="checkbox"/>	i. Home Address	<input checked="" type="checkbox"/>	o. Medical Information	<input checked="" type="checkbox"/>
d. Gender	<input checked="" type="checkbox"/>	j. Telephone Number	<input checked="" type="checkbox"/>	p. Military Service	<input type="checkbox"/>
e. Age	<input checked="" type="checkbox"/>	k. Email Address	<input checked="" type="checkbox"/>	q. Physical Characteristics	<input type="checkbox"/>
f. Race/Ethnicity	<input checked="" type="checkbox"/>	l. Education	<input type="checkbox"/>	r. Mother's Maiden Name	<input type="checkbox"/>

s. Other general personal data (specify):
-------------------------------------------

<b>Work-Related Data (WRD)</b>					
a. Occupation	<input checked="" type="checkbox"/>	d. Telephone Number	<input checked="" type="checkbox"/>	g. Salary	<input type="checkbox"/>
b. Job Title	<input checked="" type="checkbox"/>	e. Email Address	<input checked="" type="checkbox"/>	h. Work History	<input type="checkbox"/>
c. Work Address	<input checked="" type="checkbox"/>	f. Business Associates	<input type="checkbox"/>		
i. Other work-related data (specify):					

<b>Distinguishing Features/Biometrics (DFB)</b>					
a. Fingerprints	<input type="checkbox"/>	d. Photographs	<input type="checkbox"/>	g. DNA Profiles	<input type="checkbox"/>
b. Palm Prints	<input type="checkbox"/>	e. Scars, Marks, Tattoos	<input type="checkbox"/>	h. Retina/Iris Scans	<input type="checkbox"/>
c. Voice Recording/Signatures	<input type="checkbox"/>	f. Vascular Scan	<input type="checkbox"/>	i. Dental Profile	<input type="checkbox"/>
j. Other distinguishing features/biometrics (specify):					

<b>System Administration/Audit Data (SAAD)</b>					
a. User ID	<input checked="" type="checkbox"/>	c. Date/Time of Access	<input checked="" type="checkbox"/>	e. ID Files Accessed	<input type="checkbox"/>
b. IP Address	<input checked="" type="checkbox"/>	d. Queries Run	<input type="checkbox"/>	f. Contents of Files	<input type="checkbox"/>
g. Other system administration/audit data (specify):					

<b>Other Information (specify)</b>					

2.2 Indicate sources of the PII/BII in the system. (*Check all that apply.*)

<b>Directly from Individual about Whom the Information Pertains</b>					
In Person	<input type="checkbox"/>	Hard Copy: Mail/Fax	<input checked="" type="checkbox"/>	Online	<input checked="" type="checkbox"/>
Telephone	<input checked="" type="checkbox"/>	Email	<input checked="" type="checkbox"/>		
Other (specify):					

<b>Government Sources</b>					
Within the Bureau	<input type="checkbox"/>	Other DOC Bureaus	<input type="checkbox"/>	Other Federal Agencies	<input type="checkbox"/>
State, Local, Tribal	<input type="checkbox"/>	Foreign	<input type="checkbox"/>		
Other (specify):					

<b>Non-government Sources</b>					
Public Organizations	<input type="checkbox"/>	Private Sector	<input type="checkbox"/>	Commercial Data Brokers	<input type="checkbox"/>
Third Party Website or Application	<input type="checkbox"/>				
Other (specify):					

2.3 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

<b>Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)</b>			
Smart Cards	<input type="checkbox"/>	Biometrics	<input type="checkbox"/>
Caller-ID	<input type="checkbox"/>	Personal Identity Verification (PIV) Cards	<input checked="" type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.
-------------------------------------	----------------------------------------------------------------------------------------------------------

### **Section 3: System Supported Activities**

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

<b>Activities</b>			
Audio recordings	<input type="checkbox"/>	Building entry readers	<input type="checkbox"/>
Video surveillance	<input type="checkbox"/>	Electronic purchase transactions	<input type="checkbox"/>
Other (specify):			

<input checked="" type="checkbox"/>	There are not any IT system supported activities which raise privacy risks/concerns.
-------------------------------------	--------------------------------------------------------------------------------------

### **Section 4: Purpose of the System**

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

<b>Purpose</b>			
To determine eligibility	<input type="checkbox"/>	For administering human resources programs	<input checked="" type="checkbox"/>
For administrative matters	<input checked="" type="checkbox"/>	To promote information sharing initiatives	<input type="checkbox"/>
For litigation	<input type="checkbox"/>	For criminal law enforcement activities	<input type="checkbox"/>
For civil enforcement activities	<input type="checkbox"/>	For intelligence activities	<input type="checkbox"/>
To improve Federal services online	<input type="checkbox"/>	For employee or customer satisfaction	<input checked="" type="checkbox"/>
For web measurement and customization technologies (single-session )	<input type="checkbox"/>	For web measurement and customization technologies (multi-session )	<input type="checkbox"/>
Other (specify):			

## **Section 5: Use of the Information**

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

### **EEOCMRS:**

The intended use of information is to support EEOCMRS role and mission.

The information is used to manage and track EEO cases as well as to generate ad hoc and periodic reports. OEEOD staff members are allowed to search and verify EEO case records by complaint's first and last name, social security number, date of birth, case number etc.

### **RACMS:**

The information will be used to track and manage the flow of reasonable accommodation requests through the RA process from the initial filing of a new RA request to the final resolution of the request. The information will also be used to process requests for reasonable accommodation by collecting and maintaining data on accommodations requested and provided, and costs of each accommodation, for annual reporting purposes.

## **Section 6: Information Sharing and Access**

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
DOC bureaus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Federal agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
State, local, tribal gov't agencies	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Public	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Private sector	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign governments	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Foreign entities	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other (specify):	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The PII/BII in the system will not be shared.

6.2 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

<input type="checkbox"/>	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII.  <input type="checkbox"/> Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
<input checked="" type="checkbox"/>	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.3 Identify the class of users who will have access to the IT system and the PII/BII. (*Check all that apply.*)

<b>Class of Users</b>			
General Public	<input type="checkbox"/>	Government Employees	<input checked="" type="checkbox"/>
Contractors	<input type="checkbox"/>		
Other (specify):			

## **Section 7: Notice and Consent**

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. (*Check all that apply.*)

<input checked="" type="checkbox"/>	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.
<input checked="" type="checkbox"/>	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: <a href="https://www.uspto.gov/privacy-policy">https://www.uspto.gov/privacy-policy</a>
<input type="checkbox"/>	Yes, notice is provided by other means.
<input type="checkbox"/>	No, notice is not provided.

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not: This is a core requirement for being able to fully process the EEO and RA cases.

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

<input type="checkbox"/>	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
<input checked="" type="checkbox"/>	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not: The system serves a specific function, so there are no varied particular uses of PII that an individual could consent to.

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

<input checked="" type="checkbox"/>	Yes, individuals have an opportunity to review/update PII/BII pertaining to them.	Specify how: Users can request to update information through a formal process through the USPTO OHR.
<input type="checkbox"/>	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

## **Section 8: Administrative and Technological Controls**

8.1 Indicate the administrative and technological controls for the system. (*Check all that apply.*)

<input type="checkbox"/>	All users signed a confidentiality agreement or non-disclosure agreement.
<input checked="" type="checkbox"/>	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
<input checked="" type="checkbox"/>	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
<input checked="" type="checkbox"/>	Access to the PII/BII is restricted to authorized personnel only.
<input checked="" type="checkbox"/>	Access to the PII/BII is being monitored, tracked, or recorded. Explanation: The EES MicroPact and USPTO Administrator conducts monthly audits of the system, to include when and by whom the system was accessed and what info was updated, changed corrected, etc.
<input checked="" type="checkbox"/>	The information is secured in accordance with FISMA requirements. Provide date of most recent Assessment and Authorization (A&A): <u>July 25, 2016</u> <input type="checkbox"/> This is a new system. The A&A date will be provided when the A&A package is approved.
<input checked="" type="checkbox"/>	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
<input checked="" type="checkbox"/>	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POAM).
<input checked="" type="checkbox"/>	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
<input checked="" type="checkbox"/>	Contracts with customers establish ownership rights over data including PII/BII.
<input type="checkbox"/>	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
<input type="checkbox"/>	Other (specify):

## 8.2 Provide a general description of the technologies used to protect PII/BII on the IT system.

## Operational Controls:

Automated operational controls include securing all hardware associated with EES in the Micropact Data Center. The Data Center is controlled by access card entry and all use of the card is audited through the access system to restrict access to the servers, their Operating Systems and databases. In addition, physical access points to the Micropact Data Center is controlled by physical locking mechanism including separate door locks, an alarm control contact monitored twenty-four (24) hours a day, a motion detector at each door and hallway and a video camera at each hallway.

Contingency planning has been prepared for the data. Backups are performed on the processing databases. All backup tapes that contain PII or information covered under the Privacy Act are encrypted with FIPS 140-2 compliant algorithms by the MicroPact Database Administration Team.

## Technical controls:

Information is also secured through the application itself, by only allowing authorized users access to the application and to data to which they have access and privilege. Also the information system controls attacks and unauthorized attempts on the application and database through strict logins, AV protection, and through firewalls.

All data is encrypted at rest and in transit.

**Section 9: Privacy Act**

## 9.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (A new system of records notice (SORN) is required if the system is not covered by an existing SORN).

As per the Privacy Act of 1974, “the term ‘system of records’ means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.”

<input checked="" type="checkbox"/>	<p>Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name and number (<i>list all that apply</i>):</p> <p>Employees Personnel Files not covered by Notices of Other Agencies – COMMERCE/DEPT-18.</p> <p><a href="http://www.ofr.gov/(S(woq5ojwh3pljsgyh3tx0zq3q))/privacy/2011/commerce.aspx?AspxAutoDetectCookieSupport=1#dept18">http://www.ofr.gov/(S(woq5ojwh3pljsgyh3tx0zq3q))/privacy/2011/commerce.aspx?AspxAutoDetectCookieSupport=1#dept18</a></p>
<input type="checkbox"/>	<p>Yes, a SORN has been submitted to the Department for approval on <u>(date)</u>.</p>
<input type="checkbox"/>	<p>No, a SORN is not being created.</p>

## **Section 10: Retention of Information**

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. (*Check all that apply.*)

<input checked="" type="checkbox"/>	There is an approved record control schedule. Provide the name of the record control schedule:  RACMS: Yes. RACMS files that relate to reasonable accommodation request are covered by the NARA GRS Schedule 1. Civilian Personnel Records, Item 24, Reasonable Accommodation Request Records.
<input type="checkbox"/>	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
<input type="checkbox"/>	Yes, retention is monitored for compliance to the schedule.
<input checked="" type="checkbox"/>	No, retention is not monitored for compliance to the schedule. Provide explanation:  EEOCMRS: No. GRC 20 allows agency determination that certain electronic records are authorized for erasure or deletion when they are no longer needed for administrative, legal, audit, or other operational purposes. Electronic records that represent hard copy records can be deleted after expiration of the retention period authorized for the hard copy records.

10.2 Indicate the disposal method of the PII/BII. (*Check all that apply.*)

<b>Disposal</b>			
Shredding	<input type="checkbox"/>	Overwriting	<input checked="" type="checkbox"/>
Degaussing	<input type="checkbox"/>	Deleting	<input checked="" type="checkbox"/>
Other (specify):			

## **Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Levels**

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.

<input type="checkbox"/>	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
<input type="checkbox"/>	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
<input checked="" type="checkbox"/>	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact levels.  
*(Check all that apply.)*

<input checked="" type="checkbox"/>	Identifiability	Provide explanation: Detailed information of employee work related data and system administration and audit data separately or in combination may provide a detailed private individual profile.
<input type="checkbox"/>	Quantity of PII	Provide explanation:
<input type="checkbox"/>	Data Field Sensitivity	Provide explanation:
<input checked="" type="checkbox"/>	Context of Use	Provide explanation: Use of PII and work / system audit data in combination for tracking and reporting of equal employment or accommodations cases may provide a detailed private individual profile.
<input type="checkbox"/>	Obligation to Protect Confidentiality	Provide explanation:
<input checked="" type="checkbox"/>	Access to and Location of PII	Provide explanation: Because the information containing PII must be transmitted outside of the USPTO environment there is an added need to ensure the confidentiality of information during transmission.
<input type="checkbox"/>	Other:	Provide explanation:

## **Section 12: Analysis**

12.1 Indicate whether the conduct of this PIA results in any required business process changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required business process changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required business process changes.

12.2 Indicate whether the conduct of this PIA results in any required technology changes.

<input type="checkbox"/>	Yes, the conduct of this PIA results in required technology changes. Explanation:
<input checked="" type="checkbox"/>	No, the conduct of this PIA does not result in any required technology changes.